Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

# DOCENT LECTURE: Compositional Verification of Interaction Behaviour

#### Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

16 March 2007

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イヨン イヨン イヨン

3

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

**Computation**: Data Transformation + Interaction

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

- **Computation**: Data Transformation + Interaction
- **Focus on**: *on-going* interaction behaviour

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへ⊙

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

- **Computation**: Data Transformation + Interaction
- **Focus on**: *on-going* interaction behaviour
- Examples:
  - teller machine (bankomat)
  - server accepting requests and sending responses
  - applications on a mobile device interacting via method calls

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

- **Computation**: Data Transformation + Interaction
- **Focus on**: on-going interaction behaviour
- Examples:
  - teller machine (bankomat)
  - server accepting requests and sending responses
  - applications on a mobile device interacting via method calls

### Problem:

how can we reason formally about interaction behaviour?

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト 不得 トイヨト イヨト

・ ・ ロ ・ ・ 目 ・ ・ 目 ・ ・ 日 ・ ・ つ へ つ

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

#### Dynamic systems:

- components are generated dynamically
- open systems: components dynamically join and leave system

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

#### Dynamic systems:

- components are generated dynamically
- open systems: components dynamically join and leave system

#### Examples:

- concurrent server spawns off component to handle request
- application is loaded on a mobile device post-issuance

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

### Dynamic systems:

- components are generated dynamically
- open systems: components dynamically join and leave system

### Examples:

- concurrent server spawns off component to handle request
- application is loaded on a mobile device post-issuance

### Problem:

- how can we reason formally about the interaction behaviour of such systems?
- compositional reasoning needed!

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
Concurrent Serv	ver			

▲□▶ ▲□▶ ▲≧▶ ▲≧▶ = ● のへの

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

## Concurrent Server



・ロト ・ 日 ・ ・ ヨ ・ ・ ヨ ・

3

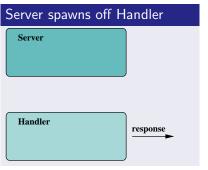
Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

### Concurrent Server





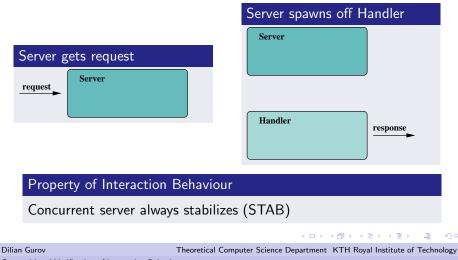
イロン イ理ト イヨト イヨト

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
	00	000	
	Interaction Behaviour	00	

### Concurrent Server



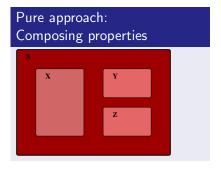
Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

▲□▶ ▲圖▶ ▲国▶ ▲国▶ ▲国 ● ○○○

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

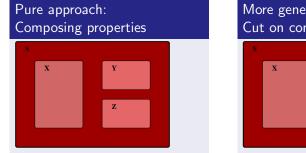


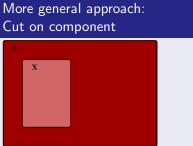
Theoretical Computer Science Department KTH Royal Institute of Technology

<ロ> (日) (日) (日) (日) (日)

Compositional Verification of Interaction Behaviour

Dilian Gurov

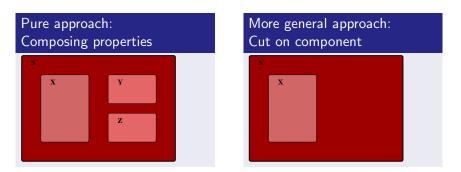




Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト



### Concurrent Server

### How does compositional reasoning help?

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

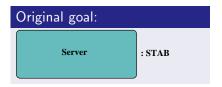
イロト イヨト イヨト イヨト

# Proving Stabilization of Concurrent Server

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

# Proving Stabilization of Concurrent Server

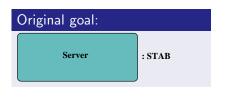


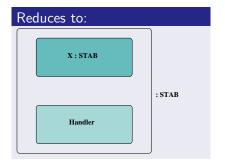
Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト

Dilian Gurov

# Proving Stabilization of Concurrent Server





・ロト ・ 理 ト ・ 国 ト ・ 国 ト ・

3

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
0				

## Overview

- 1 Framework for Formal Reasoning
- 2 Interaction Behaviour
- 3 Behavioural Properties
  - Specification
  - Verification
- 4 Compositional VerificationProof Systems
  - Maximal Models

### 5 Conclusion

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

<ロ> (日) (日) (日) (日) (日)

- ・ロト ・ 聞 ト ・ ヨト ・ ヨー ・ りゃつ

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

#### Semantic Domains for Interaction Behaviour

- function from initial to final states: not suitable
- rather: sequences, or even trees, of interactions

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イ理ト イヨト イヨト

3

#### Semantic Domains for Interaction Behaviour

- function from initial to final states: not suitable
- rather: sequences, or even trees, of interactions

### Defining Interaction Behaviour

- semantic domain too low-level and unstructured
- composing behaviours
- meaning of behavioural definition given in semantic domain

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

#### Specification and Verification

- specification captures desired behaviour
- verification establishes whether model/implementation meets specification

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イヨン イヨン イヨン

#### Specification and Verification

- specification captures desired behaviour
- verification establishes whether model/implementation meets specification

### Compositional Verification

inferring system properties from component properties

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

#### Semantic Domains

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

▲ロト ▲圖ト ▲国ト ▲国ト 三連

Framework for Formal F	Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

### Semantic Domains

Traces (or runs, executions, paths)

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

★ロト ★御 と★ ヨ と ★ ヨ と 三 ヨ

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

### Semantic Domains

- Traces (or runs, executions, paths)
- Computation trees

Theoretical Computer Science Department KTH Royal Institute of Technology

▲口▶ ▲圖▶ ▲理▶ ▲理▶

Compositional Verification of Interaction Behaviour

Dilian Gurov

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000	

### Semantic Domains

- Traces (or runs, executions, paths)
- Computation trees
- Labelled Transition Systems (LTS)

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イヨン イヨン イヨン

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000	

#### Semantic Domains

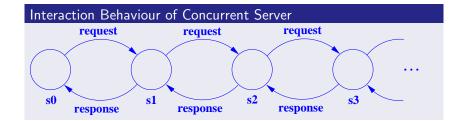
- Traces (or runs, executions, paths)
- Computation trees
- Labelled Transition Systems (LTS)
- Modal Transition Systems

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イヨン イヨン イヨン

# LTS Example: Concurrent Server



・ロト・西ト・西ト・西ト 前 ろくの

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

### Defining Interaction Behaviour

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000 000	

#### Defining Interaction Behaviour

Process Algebra: Calculus of Communicating Systems

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト 不問 とくほど 不良とう 酒

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

#### Defining Interaction Behaviour

- Process Algebra: Calculus of Communicating Systems
- Programming language: Erlang

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト 不問 とくほど 不良とう 酒

Compositional Verification of Interaction Behaviour

Dilian Gurov

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

## Interaction Behaviour

#### Defining Interaction Behaviour

- Process Algebra: Calculus of Communicating Systems
- Programming language: Erlang
- Control Flow Graph: extracted from Java bytecode

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

(日) (圖) (E) (E) (E)

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000	

## Interaction Behaviour

#### Defining Interaction Behaviour

- Process Algebra: Calculus of Communicating Systems
- Programming language: Erlang
- Control Flow Graph: extracted from Java bytecode

### LTS Semantics

Induced by transition rules

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

(日) (圖) (E) (E) (E)

# Calculus of Communicating Systems (CCS)

- ・ロト・(聞)・ (目)・ (目)・ (目)・ (の)

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

# Calculus of Communicating Systems (CCS)

## CCS Syntax

$$E ::= \mathbf{0} \mid A \mid \alpha . E \mid E + E \mid E \mid E$$

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト

3

# Calculus of Communicating Systems (CCS)

## CCS Syntax

$$E ::= \mathbf{0} \mid A \mid \alpha . E \mid E + E \mid E \mid E$$

### CCS Semantics: Transition Rules (induce LTS)

PREFIX 
$$\xrightarrow{-}{\alpha.E \xrightarrow{\alpha} E}$$
 DEF  $\xrightarrow{E \xrightarrow{\alpha} F} A \stackrel{\Delta}{=} E$   
CHOICE  $\xrightarrow{E \xrightarrow{\alpha} E'} E'$  COMM  $\xrightarrow{E \xrightarrow{\alpha} E'} E|F \xrightarrow{\alpha} E'|F$ 

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

3

			leasoning

Interaction Behaviour

# CCS Example: Concurrent Server

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

## CCS Example: Concurrent Server

### Defining Concurrent Server

$$CServer \stackrel{\Delta}{=} request.(CServer \mid response.\mathbf{0})$$

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

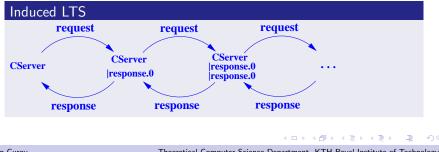
イロト イヨト イヨト イヨト

3

## CCS Example: Concurrent Server

### Defining Concurrent Server

$$CServer \stackrel{\Delta}{=} request.(CServer \mid response.\mathbf{0})$$



Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Conclusion

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		•O 00	000	

# Specifying Behavioural Properties

### Specifying Sets of Behaviours

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イヨン イヨン イヨン

3

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties •0 00	Compositional Verification	Conclusion
C 10 11				

## Specifying Behavioural Properties

### Specifying Sets of Behaviours

Modal logic: Hennessy-Milner Logic (HML)

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イ理ト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties •0 00	Compositional Verification	Conclusion

# Specifying Behavioural Properties

### Specifying Sets of Behaviours

- Modal logic: Hennessy-Milner Logic (HML)
- Temporal logic: Computation Tree Logic (CTL)

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000	

# Specifying Behavioural Properties

### Specifying Sets of Behaviours

- Modal logic: Hennessy-Milner Logic (HML)
- Temporal logic: Computation Tree Logic (CTL)
- Modal  $\mu$ -calculus: HML + Recursion ( $\mu$ K)

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		<b>O</b> O	000	

# Specifying Behavioural Properties

### Specifying Sets of Behaviours

- Modal logic: Hennessy-Milner Logic (HML)
- Temporal logic: Computation Tree Logic (CTL)
- Modal  $\mu$ -calculus: HML + Recursion ( $\mu$ K)

#### Example: Formalizing STAB

CTL: AG (AF stab)

Theoretical Computer Science Department KTH Royal Institute of Technology

Dilian Gurov

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000	

# Specifying Behavioural Properties

### Specifying Sets of Behaviours

- Modal logic: Hennessy-Milner Logic (HML)
- Temporal logic: Computation Tree Logic (CTL)
- Modal  $\mu$ -calculus: HML + Recursion ( $\mu$ K)

#### Example: Formalizing STAB

• CTL: AG (AF stab) •  $\mu$ K:  $\nu X. \mu Y.$  [request]  $X \wedge$  [-request] Y

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

(日)

# Hennessy-Milner Logic (HML)

・ロト・個ト・目下・目下 油 のくの

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties ○● ○○	Compositional Verification	Conclusion
Specification				

# Hennessy-Milner Logic (HML)

## HML Syntax

## $\Phi ::= \mathbf{t} \mathbf{t} \mid \mathbf{f} \mid \Phi \lor \Phi \mid \Phi \land \Phi \mid \langle \alpha \rangle \Phi \mid [\alpha] \Phi$

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへ⊙

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties ○● ○○	Compositional Verification	Conclusion
Specification				

# Hennessy-Milner Logic (HML)

## HML Syntax

$$\Phi ::= \mathbf{t} \mathbf{t} | \mathbf{f} \mathbf{f} | \Phi \lor \Phi | \Phi \land \Phi | \langle \alpha \rangle \Phi | [\alpha] \Phi$$

### HML Semantics: Satisfaction Relation $s \models^{\mathcal{T}} \Phi$

$$\begin{array}{ll} s \models^{\mathcal{T}} \langle \alpha \rangle \, \Phi & \stackrel{\mathsf{def}}{\Leftrightarrow} & \exists s' \in \mathcal{S}. \ (s \stackrel{\alpha}{\longrightarrow} s' \wedge s' \models^{\mathcal{T}} \Phi) \\ s \models^{\mathcal{T}} [\alpha] \, \Phi & \stackrel{\mathsf{def}}{\Leftrightarrow} & \forall s' \in \mathcal{S}. \ (s \stackrel{\alpha}{\longrightarrow} s' \Rightarrow s' \models^{\mathcal{T}} \Phi) \end{array}$$

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イ理ト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000	

## Verifying Behavioural Properties: Interactive

・ ・ ・ ・ 「 ・ ・ = ・ ・ = ・ うへの

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	
		•••	0000	

Dilian Gurov

## Verifying Behavioural Properties: Interactive

Proof System Based: Judgements  $s \vdash^{\mathcal{T}} \Phi$ 

$$\text{TRUE} \frac{-}{s \vdash^{T} \mathbf{tt}} \quad \text{ORL} \frac{s \vdash^{T} \Phi}{s \vdash^{T} \Phi \lor \Psi} \quad \text{ORR} \frac{s \vdash^{T} \Psi}{s \vdash^{T} \Phi \lor \Psi}$$

$$\text{AND} \frac{s \vdash^{T} \Phi}{s \vdash^{T} \Phi \land \Psi} \quad \text{DIA} \frac{s' \vdash^{T} \Phi}{s \vdash^{T} \langle \alpha \rangle \Phi} s' \in \partial_{\alpha}(s)$$

$$\text{Box} \frac{s_{1} \vdash^{T} \Phi \dots s_{n} \vdash^{T} \Phi}{s \vdash^{T} [\alpha] \Phi} \partial_{\alpha}(s) = \{s_{1}, \dots, s_{n}\}$$

Theoretical Computer Science Department KTH Royal Institute of Technology

・ロト ・ 日 ・ ・ ヨ ト ・ ヨ ト ・

# Verifying Behavioural Properties: Algorithmic

Model Checking  $s \models^{\mathcal{T}} \Phi$ 

▲□▶▲圖▶▲圖▶▲圖▶ 圖 の()

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

## Verifying Behavioural Properties: Algorithmic

Model Checking  $s \models^{\mathcal{T}} \Phi$ 

 local techniques: execute s guided by Φ proof strategies give rise to MC algorithms

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

・ロト ・ 日 ・ ・ ヨ ト ・ ヨ ト ・

## Verifying Behavioural Properties: Algorithmic

## Model Checking $s \models^{\mathcal{T}} \Phi$

- local techniques: execute s guided by Φ proof strategies give rise to MC algorithms
- **global** techniques: compute all Φ-states, check membership

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

## Verifying Behavioural Properties: Algorithmic

## Model Checking $s \models^{\mathcal{T}} \Phi$

- local techniques: execute s guided by Φ proof strategies give rise to MC algorithms
- **global** techniques: compute all Φ-states, check membership

### Complexity of Model Checking

 For Finite–State Systems: polynomial in size of model, exponential in size of formula

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

# Verifying Behavioural Properties: Algorithmic

## Model Checking $s \models^{\mathcal{T}} \Phi$

- local techniques: execute s guided by Φ proof strategies give rise to MC algorithms
- **global** techniques: compute all Φ-states, check membership

### Complexity of Model Checking

- For Finite–State Systems:
  - polynomial in size of model, exponential in size of formula
- For Pushdown Automata: exponential in number of non-terminals and in size of formula

Dilian Gurov

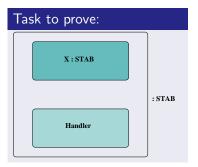
Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000	

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	



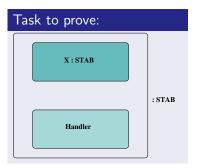
Theoretical Computer Science Department KTH Royal Institute of Technology

・ロト ・ 日 ・ ・ ヨ ・ ・ ヨ ・

3

Compositional Verification of Interaction Behaviour

Dilian Gurov



### Notation:

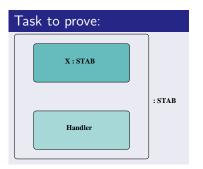
## $X : STAB \models X | Handler : STAB$

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

・ロト ・ 日 ト ・ ヨ ト ・ ヨ ト

3



#### Notation:

 $X : \mathsf{STAB} \models X | \mathsf{Handler} : \mathsf{STAB}$ 

### Approaches:

- Interactive: proof systems
- Algorithmic: maximal models

<ロ> (日) (日) (日) (日) (日)

3

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

## Proof System for Compositional Verification

- ・ロト・日本・ キャー キャー キー ろくの

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
Proof Systems				

## Proof System for Compositional Verification

#### Judgements

 $\Gamma \vdash \Delta$  where  $\Gamma$ ,  $\Delta$  are sets of assertions

▲□▶ ▲□▶ ▲目▶ ▲目▶ 三目 - 釣�(

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
Due of Suntaine				

## Proof System for Compositional Verification

Judgements			
$\Gamma \vdash \Delta$ whe	ere Γ, $\Delta$ are	sets of assertions	
Term Cut Rule	9		
TermCut	$\vdash C : \Phi$	$X: \Phi \vdash X   E: \Psi$ $- C   E: \Psi$	_
1 1100 0 0 1	ŀ	- C E : Ψ	

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イヨト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
D (C)				

## Proof System for Compositional Verification

Judgements	
$\Gamma \vdash \Delta$ whe	re $\Gamma$ , $\Delta$ are sets of assertions
Term Cut Rule	
TermCut	$ \vdash C : \Phi \qquad X : \Phi \vdash X   E : \Psi \\ \vdash C   E : \Psi $
	$\vdash C E: \Psi$

#### Global Discharge Rule

- explicit ordinal approximation
- proof tree embodies a valid proof by well-founded induction
- powerful mechanism for inductive and co-inductive proofs

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

## Proving Stabilization of Concurrent Server

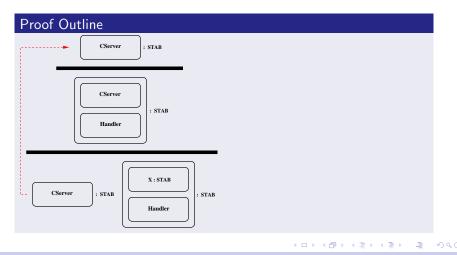
- ・ロト・日本・日本・日本・日本・今日や

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification ○●○ ○○○	Conclusion

# Proving Stabilization of Concurrent Server



Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Conclusion

Proof Systems

# Proof System for Compositional Verification

### Properties

- ・ロト・(部)ト・ヨト・ヨト ヨー のの(

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

# Proof System for Compositional Verification

### Properties

sound: only valid judgements are derivable

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

<ロ> (日) (日) (日) (日) (日)

Proof Systems

# Proof System for Compositional Verification

### Properties

- sound: only valid judgements are derivable
- incomplete in general: even X : Φ, Y : Ψ ⊨ X|Y : Θ is undecidable for μK!

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

Proof Systems

# Proof System for Compositional Verification

### Properties

- sound: only valid judgements are derivable
- incomplete in general: even X : Φ, Y : Ψ ⊨ X|Y : Θ is undecidable for μK!
- complete for logic fragment: only variables as terms

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

(a)

Proof Systems

Dilian Gurov

# Proof System for Compositional Verification

### Properties

- sound: only valid judgements are derivable
- incomplete in general: even X : Φ, Y : Ψ ⊨ X|Y : Θ is undecidable for μK!
- complete for logic fragment: only variables as terms
- complete for model checking fragment: closed, regular CCS terms

Theoretical Computer Science Department KTH Royal Institute of Technology

(a)

Proof Systems

# Proof System for Compositional Verification

### Properties

- sound: only valid judgements are derivable
- incomplete in general: even X : Φ, Y : Ψ ⊨ X|Y : Θ is undecidable for μK!
- complete for logic fragment: only variables as terms
- complete for model checking fragment: closed, regular CCS terms
- complete for pushdown automata

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
Maximal Models				

Under certain conditions...

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification ○○○ ●○○	Conclusion
Maximal Models				

#### Under certain conditions...



Theoretical Computer Science Department KTH Royal Institute of Technology

・ロト ・ 理ト ・ ヨト ・ ヨト

3

Dilian Gurov

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
Maximal Models				

### Under certain conditions...



Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イヨン イヨン イヨン

3

Compositional Verification of Interaction Behaviour

Dilian Gurov

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	
Maximal Models				

#### Conditions

There is a (simulation) pre-order  $\leq$  on components:

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト 不問 とくほど 不良とう 酒

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
Maximal Madala				

### Maximal Models for Compositional Verification

#### Conditions

There is a (simulation) pre-order  $\leq$  on components:

**1** property preserving:

 $C_1 \leq C_2$  and  $\models C_2 : \Phi$  imply  $\models C_1 : \Phi$ 

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト 不問 とくほど 不良とう 酒

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	
		00	000	
NA 1 1 NA 1 1				

## Maximal Models for Compositional Verification

### Conditions

There is a (simulation) pre–order  $\leq$  on components:

 property preserving: C<sub>1</sub> ≤ C<sub>2</sub> and ⊨ C<sub>2</sub> : Φ imply ⊨ C<sub>1</sub> : Φ
 preserved by composition:

 $C_1 \leq C_2$  implies  $C_1 | C_3 \leq C_2 | C_3$ 

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

(日) (圖) (E) (E) (E)

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
NA 1 1 NA 1 1				

### Maximal Models for Compositional Verification

### Conditions

There is a (simulation) pre–order  $\leq$  on components:

#### **1** property preserving:

 $C_1 \leq C_2$  and  $\models C_2 : \Phi$  imply  $\models C_1 : \Phi$ 

**2** preserved by composition:

$$C_1 \leq C_2$$
 implies  $C_1 | C_3 \leq C_2 | C_3$ 

3 the set of  $\Phi$ -components has a maximal element w.r.t.  $\leq$ 

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

(日) (圖) (E) (E) (E)

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

### Maximal Models for Compositional Verification

### Conditions

There is a (simulation) pre–order  $\leq$  on components:

#### **1** property preserving:

 $C_1 \leq C_2 \text{ and } \models C_2 : \Phi \text{ imply } \models C_1 : \Phi$ 

**2** preserved by composition:

$$C_1 \leq C_2$$
 implies  $C_1 | C_3 \leq C_2 | C_3$ 

3 the set of  $\Phi$ -components has a maximal element w.r.t.  $\leq$ 

#### Maximal Model Principle

$$[OD \quad \frac{\models Max(\Phi)|E:\Psi}{X:\Phi\models X|E:\Psi}$$

Dilian Gurov

MAXM

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト イポト イヨト イヨト

-

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00 00	000 000	
Maximal Models				

Derived Compositional Verification Principle			
Compos	$\models C : \Phi$	$\models Max(\Phi) E: \Psi$	
COMPOS		= C E : Ψ	

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

▲白▶ ▲圖▶ ▲臣▶ ▲臣▶

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion
Maximal Models				

Derived Com			
Compos	$\models C : \Phi$	$ \models Max(\Phi) E:\Psi $ $ \models C E:\Psi $	

1 ACTL (Kripke models)

Applies to:

- 2 Simulation Logic (Control Flow Graphs)
- **3** modal  $\mu$ -calculus (EMTS)

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

ヘロト 人間 ト くほ ト くほ トー

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

### Interaction Behaviour

Interaction behaviour can be:

▲□▶▲圖▶▲≣▶▲≣▶ ≣ ∽९९(

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

#### Interaction Behaviour

Interaction behaviour can be:

captured elegantly through LTS

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イヨン イヨン イヨン

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000 000	

#### Interaction Behaviour

Interaction behaviour can be:

- captured elegantly through LTS
- defined in various ways: CCS, Erlang, Control Flow Graphs

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロン イ理ト イヨト イヨト

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000 000	

#### Interaction Behaviour

Interaction behaviour can be:

- captured elegantly through LTS
- defined in various ways: CCS, Erlang, Control Flow Graphs
- specified in various logics: HML, CTL,  $\mu$ K

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

イロト 不問 とくほど 不良とう 酒

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000 000	

#### Interaction Behaviour

Interaction behaviour can be:

- captured elegantly through LTS
- defined in various ways: CCS, Erlang, Control Flow Graphs
- $\blacksquare$  specified in various logics: HML, CTL,  $\mu K$
- verified algorithmically or interactively

Theoretical Computer Science Department KTH Royal Institute of Technology

ヘロト 人間 ト くほ ト くほ トー

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

#### Interaction Behaviour

Interaction behaviour can be:

- captured elegantly through LTS
- defined in various ways: CCS, Erlang, Control Flow Graphs
- specified in various logics: HML, CTL,  $\mu K$
- verified algorithmically or interactively

### Compositional Verification

good for modular design

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

#### Interaction Behaviour

Interaction behaviour can be:

- captured elegantly through LTS
- defined in various ways: CCS, Erlang, Control Flow Graphs
- $\blacksquare$  specified in various logics: HML, CTL,  $\mu K$
- verified algorithmically or interactively

### Compositional Verification

- good for modular design
- needed for verifying open systems

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

#### Interaction Behaviour

Interaction behaviour can be:

- captured elegantly through LTS
- defined in various ways: CCS, Erlang, Control Flow Graphs
- $\blacksquare$  specified in various logics: HML, CTL,  $\mu K$
- verified algorithmically or interactively

### Compositional Verification

- good for modular design
- needed for verifying open systems
- algorithmically or interactively

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties 00 00	Compositional Verification	Conclusion

### Future Challenges

・ キョット 4 回 ア・ 4 回 ア・ 4 回 ア・ 1

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

### Future Challenges

#### Interactive Verification

How to reason about *complex phenomena* such as:

- failure and recovery
- self-stabilization
- in open, dynamic systems?

Theoretical Computer Science Department KTH Royal Institute of Technology

<ロ> (日) (日) (日) (日) (日)

Compositional Verification of Interaction Behaviour

Dilian Gurov

Framework for Formal Reasoning	Interaction Behaviour	Behavioural Properties	Compositional Verification	Conclusion
		00	000	

### Future Challenges

#### Interactive Verification

How to reason about *complex phenomena* such as:

- failure and recovery
- self-stabilization
- in open, dynamic systems?

#### Algorithmic Verification

How to achieve scalability of verification?

- separating concerns
- abstraction mechanisms

Dilian Gurov

Theoretical Computer Science Department KTH Royal Institute of Technology

(a) < ((a) <